Exam : SC-200

Title : Microsoft Security Operations Analyst

https://www.passcert.com/SC-200.html

1. Topic 1, Contoso Ltd

Case study
This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview
A company named Contoso Ltd. has a main office and five branch offices located throughout North America. The main office is in Seattle. The branch offices are in Toronto, Miami, Houston, Los Angeles, and Vancouver.
Contoso has a subsidiary named Fabrikam, Ltd. that has offices in New York and San Francisco.

Existing Environment
End-User Environment
All users at Contoso use Windows 10 devices. Each user is licensed for Microsoft 365. In addition, iOS devices are distributed to the members of the sales team at Contoso.

Cloud and Hybrid Infrastructure
All Contoso applications are deployed to Azure.
You enable Microsoft Cloud App Security.
Contoso and Fabrikam have different Azure Active Directory (Azure AD) tenants. Fabrikam recently purchased an Azure subscription and enabled Azure Defender for all supported resource types.

Current Problems
The security team at Contoso receives a large number of cybersecurity alerts. The security team spends

too much time identifying which cybersecurity alerts are legitimate threats, and which are not.

The Contoso sales team uses only iOS devices. The sales team members exchange files with customers by using a variety of third-party tools. In the past, the sales team experienced various attacks on their devices.

The marketing team at Contoso has several Microsoft SharePoint Online sites for collaborating with external vendors. The marketing team has had several incidents in which vendors uploaded files that contain malware.

The executive team at Contoso suspects a security breach. The executive team requests that you identify which files had more than five activities during the past 48 hours, including data access, download, or deletion for Microsoft Cloud App Security-protected applications.

Requirements
Planned Changes
Contoso plans to integrate the security operations of both companies and manage all security operations centrally.

Technical Requirements
Contoso identifies the following technical requirements:
➪ Receive alerts if an Azure virtual machine is under brute force attack.
➪ Use Azure Sentinel to reduce organizational risk by rapidly remediating active attacks on the environment.
➪ Implement Azure Sentinel queries that correlate data across the Azure AD tenants of Contoso and Fabrikam.
➪ Develop a procedure to remediate Azure Defender for Key Vault alerts for Fabrikam in case of external attackers and a potential compromise of its own Azure AD applications.
➪ Identify all cases of users who failed to sign in to an Azure resource for the first time from a given country. A junior security administrator provides you with the following incomplete query.

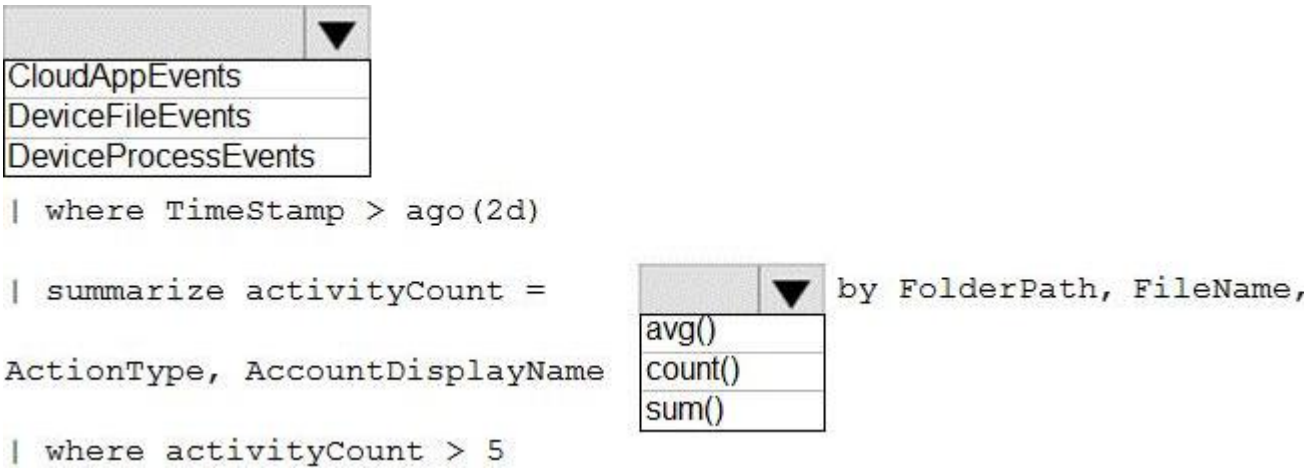
```
BehaviorAnalytics
| where ActivityType == "FailedLogOn"
| where _____ == True
```

You need to remediate active attacks to meet the technical requirements.
What should you include in the solution?
A. Azure Automation runbooks
B. Azure Logic Apps
C. Azure Functions
D Azure Sentinel livestreams
Answer: B
Explanation:
Reference: https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks

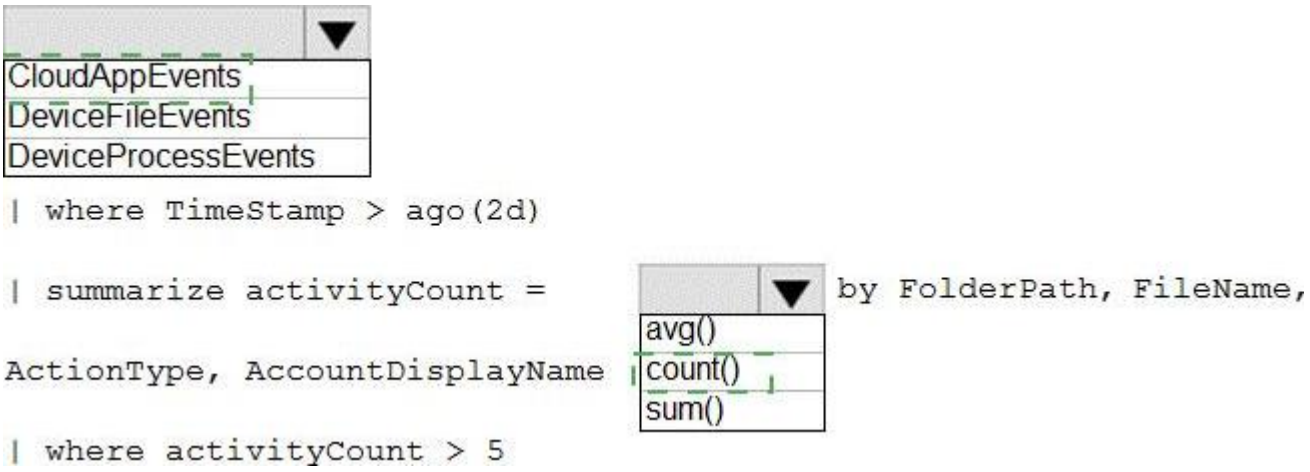
2.HOTSPOT

You need to create an advanced hunting query to investigate the executive team issue.

How should you complete the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer:

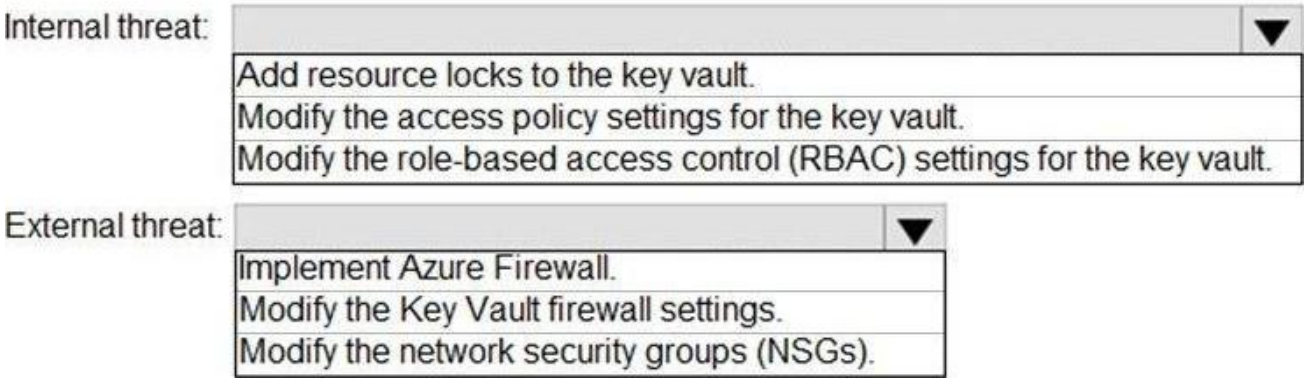


3.HOTSPOT

You need to recommend remediation actions for the Azure Defender alerts for Fabrikam.

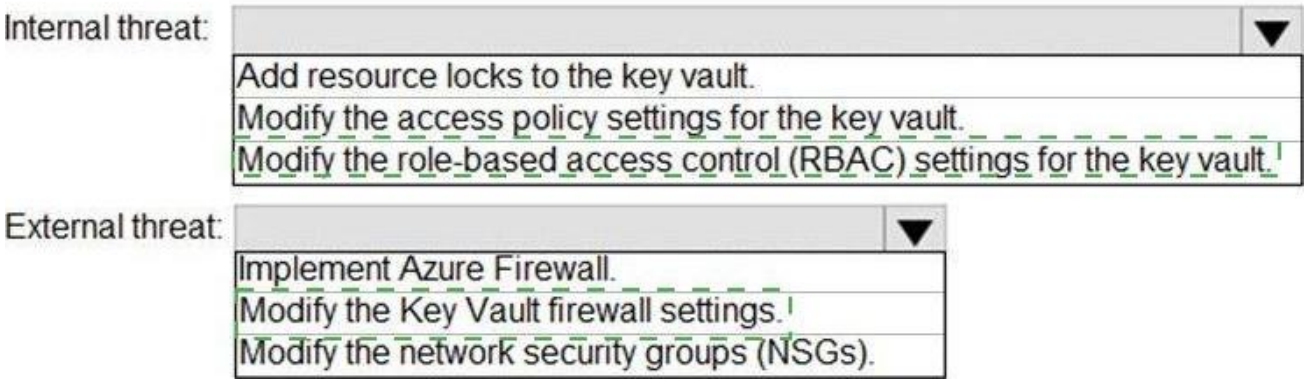
What should you recommend for each threat? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area


Internal threat:
Add resource locks to the key vault.
Modify the access policy settings for the key vault.
Modify the role-based access control (RBAC) settings for the key vault.
External threat:
Implement Azure Firewall.
Modify the Key Vault firewall settings.
Modify the network security groups (NSGs).

Answer:

Answer Area


Internal threat:
Add resource locks to the key vault.
Modify the access policy settings for the key vault.
Modify the role-based access control (RBAC) settings for the key vault.
External threat:
Implement Azure Firewall.
Modify the Key Vault firewall settings.
Modify the network security groups (NSGs).

4.You need to recommend a solution to meet the technical requirements for the Azure virtual machines.
What should you include in the recommendation?
A. just-in-time (JIT) access
B. Azure Defender
C. Azure Firewall
D. Azure Application Gateway
Answer: B
Explanation:
Reference: https://docs.microsoft.com/en-us/azure/security-center/azure-defender

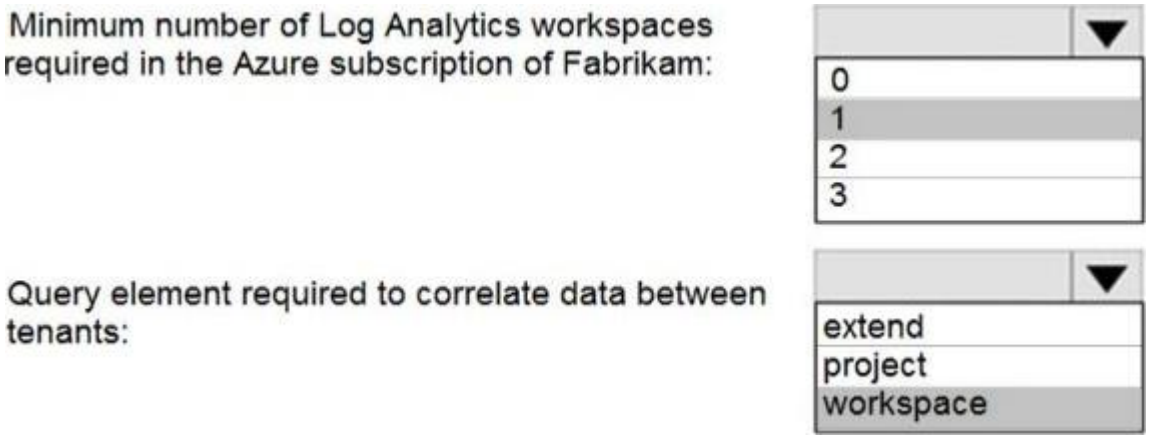
5.You need to complete the query for failed sign-ins to meet the technical requirements.
Where can you find the column name to complete the where clause?
A. Security alerts in Azure Security Center
B. Activity log in Azure
C. Azure Advisor
D. the query windows of the Log Analytics workspace

Answer: D

6.The issue for which team can be resolved by using Microsoft Defender for Office 365?
A. executive
B. marketing
C. security
D. sales
Answer: B
Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-for-spo-odb-and-teams?view=o365-worldwide

7.HOTSPOT
You need to implement Azure Sentinel queries for Contoso and Fabrikam to meet the technical requirements.
What should you include in the solution? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:



8.The issue for which team can be resolved by using Microsoft Defender for Endpoint?
A. executive

B. sales
C. marketing
Answer: B
Explanation:
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-atp-ios

9. Topic 2, Litware inc.

Case study
This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview
Litware Inc. is a renewable company.
Litware has offices in Boston and Seattle. Litware also has remote users located across the United States. To access Litware resources, including cloud resources, the remote users establish a VPN connection to either office.

Existing Environment
Identity Environment
The network contains an Active Directory forest named litware.com that syncs to an Azure Active Directory (Azure AD) tenant named litware.com.

Microsoft 365 Environment

Litware has a Microsoft 365 E5 subscription linked to the litware.com Azure AD tenant. Microsoft Defender for Endpoint is deployed to all computers that run Windows 10. All Microsoft Cloud App Security built-in anomaly detection policies are enabled.

Azure Environment

Litware has an Azure subscription linked to the litware.com Azure AD tenant.

The subscription contains resources in the East US Azure region as shown in the following table.

Name	Type	Description
LA1	Log Analytics workspace	Contains logs and metrics collected from all Azure resources and on-premises servers
VM1	Virtual machine	Server that runs Windows Server 2019
VM2	Virtual machine	Server that runs Ubuntu 18.04 LTS

Network Environment

Each Litware office connects directly to the internet and has a site-to-site VPN connection to the virtual networks in the Azure subscription.

On-premises Environment

The on-premises network contains the computers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller in litware.com that connects directly to the internet
CLIENT1	Windows 10	Boston	Domain-joined client computer

Current problems

Cloud App Security frequently generates false positive alerts when users connect to both offices simultaneously.

Planned Changes

Litware plans to implement the following changes:

- Create and configure Azure Sentinel in the Azure subscription.
- Validate Azure Sentinel functionality by using Azure AD test user accounts.

Business Requirements

Litware identifies the following business requirements:

-The principle of least privilege must be used whenever possible.

-Costs must be minimized, as long as all other requirements are met.

-Logs collected by Log Analytics must provide a full audit trail of user activities.

-All domain controllers must be protected by using Microsoft Defender for Identity.

Azure Information Protection Requirements

All files that have security labels and are stored on the Windows 10 computers must be available from the Azure Information Protection – Data discovery dashboard.

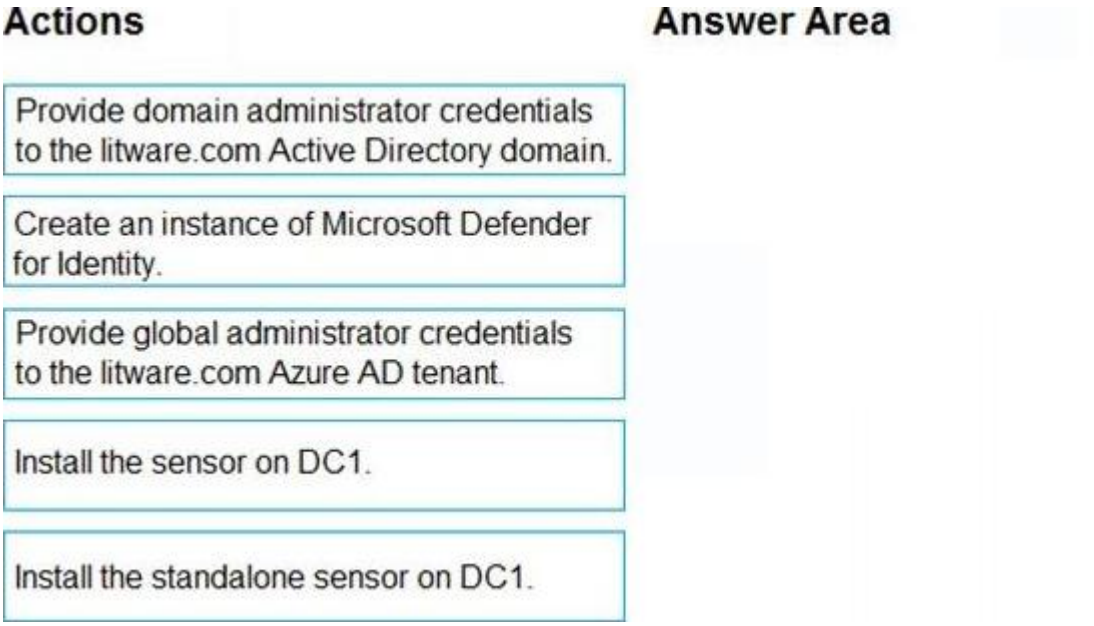
Microsoft Defender for Endpoint requirements
All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.

Microsoft Cloud App Security requirements
Cloud App Security must identify whether a user connection is anomalous based on tenant-level data.

Azure Defender Requirements
All servers must send logs to the same Log Analytics workspace.

Azure Sentinel Requirements
Litware must meet the following Azure Sentinel requirements:
- Integrate Azure Sentinel and Cloud App Security.
- Ensure that a user named admin1 can configure Azure Sentinel playbooks.
- Create an Azure Sentinel analytics rule based on a custom query. The rule must automatically initiate the execution of a playbook.
- Add notes to events that represent data access from a specific IP address to provide the ability to reference the IP address when navigating through an investigation graph while hunting.
- Create a test rule that generates alerts when inbound access to Microsoft Office 365 by the Azure AD test user accounts is detected. Alerts generated by the rule must be grouped into individual incidents, with one incident per test user account.

DRAG DROP
You need to configure DC1 to meet the business requirements.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.


Actions
Answer Area
Provide domain administrator credentials to the litware.com Active Directory domain.
Create an instance of Microsoft Defender for Identity.
Provide global administrator credentials to the litware.com Azure AD tenant.
Install the sensor on DC1.
Install the standalone sensor on DC1.

Answer:

Actions	Answer Area
Provide domain administrator credentials to the litware.com Active Directory domain.	Provide global administrator credentials to the litware.com Azure AD tenant.
Create an instance of Microsoft Defender for Identity.	Create an instance of Microsoft Defender for Identity.
Provide global administrator credentials to the litware.com Azure AD tenant.	Provide domain administrator credentials to the litware.com Active Directory domain.
Install the sensor on DC1.	Install the sensor on DC1.
Install the standalone sensor on DC1.	

Explanation:

Text

Description automatically generated with medium confidence

Step 1: log in to https://portal.atp.azure.com as a global admin

Step 2: Create the instance

Step 3. Connect the instance to Active Directory

Step 4. Download and install the sensor.